REMARKS

Claim 36 has been amended and claim 37 has been added. Hence, claims 1 – 37 are pending in the application.

FIGS. 1 and 2 have been amended to correct margin errors.

Summary of the Office Action

The Office Action has been made final even though it is the first one in this case [sic] and because all claims are drawn to the same invention earlier claimed and could have been rejected, in the next Office Action, on the grounds and art of record.

The disclosure was objected to because, on page 15, line 8 of the specification, the term "element 272" is indefinite. As mentioned in the previous Office Action, the Applicant has reviewed this section of the specification and the related drawings and is unable to determine why the Office Action has found the term to be indefinite. The Office Action statements regarding this rejection are only conclusory because it states no basis for indefiniteness. Further clarification is requested.

Claims 6 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter claimed.

Claims 1 – 12, 15 – 19, 26 – 32 are rejected under 35 USC 103(a) as being unpatentable over U.S. Publication No. 2002/0016824, herein Leeds, in view of U.S. Patent No. 6,161,130, herein Horvitz.

Claims 12, 13, 14 and 20 are rejected under 35 *USC* 103(a) as being unpatentable over Leeds in view of U.S. Publication No. 2002/0016916, herein Natarajan. These rejections are traversed.

Claims 21 – 25, 33 and 34 are rejected under 35 *USC* 103(a) as being unpatentable over Leeds in view of U.S. Publication No. 2002/0026634, herein Shaw.

FINALITY OF OFFICE ACTION

Applicant respectfully requests withdrawal of the finality of the Office Action. Based on a position taken by an Advisory Action, all the claims are, in fact, not drawn to the exact same invention, and therefore issuance of a Final Action is not proper. Specifically, the Advisory Action alleged that the argument made by Applicant in the previous response for claims 1 and 26 argued limitations not supported by the claims, that is, relies on the assertion in the argument that the claims require the limitation of "automatically determines what particular content to use to classify electronic mail messages" as being the particular limitation not in claims 1 and 26. To clearly obviate this allegation, a new claim 35 was provided, the new claim 35 not only including the limitations of claims 1 and 26 but the limitation allegedly missing (see lines 5 and 6 of claim 3). Thus, Applicant's submission for the last Request for Continued Examination added a claim limitation that the Advisory Action previously stated was missing and not in the previously pending claims. Thus, based on the position taken by the Advisory Action, the claims contain a claim with a new limitation and are not drawn to the exact same invention.

REJECTIONS BASED ON 35 USC 112

Claims 6 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter claimed because the term is "signature element" is a relative term, the specification does not provide a standard for ascertaining the requisite degree of certainty, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

In the previous Response, Applicant noted that not only does the specification describe, in detail, how the signatures are used, but also describes, in detail, various examples of how they are made. Given all the detail provided for how the signature elements can be used and how they

14

can be made, one skilled in the art would be sufficiently apprised of the scope of the claims to the extent required by 35 USC 112.

The Office Action re-iterates the arguments about this rejection made in earlier Office Actions, except that the Office Action asks the Applicant where in the specification does it show in detail how signatures are used and made. The following passage provides detailed examples of how signature elements are made.

Signature generator 120 generates message signature 260, which may include one or more signature elements 270. In one embodiment of the present invention, signature generator 120 generates one or more signature elements 270 by applying a one way hash function to a portion of electronic mail message 210. For example, signature generator 120 may read data from a portion of body part 232, and apply a first one-way hash function to the read data to produce element 272. Likewise, signature generator 120 may read data from a portion of body part 234, and apply a second hash function to produce element 274.

Alternatively, signature generator 120 may read portions of multiple body parts within electronic mail message 210, apply a hash value function to the read data to generate element 272. Likewise, signature generator 120 may read other portions of multiple body parts within electronic mail message 210, and apply a hash function to the read data to generate element 274. (beginning at page 15, line 4)

For an example of a detailed description of the use of signature elements, Applicant refers to the section "IDENTIFYING BULKMAIL BASED ON COUNTS", beginning on line 8, page 16).

Reconsideration and removal of this rejection is respectfully requested.

15

REJECTIONS BASED ON PRIOR ART

CLAIM 35

Claim 35 recites:

automatically generating a set of criteria based on contents of a plurality of electronic

mail messages received over a network;

wherein the step of automatically generating a set of criteria includes

in response to determining that a threshold number of said plurality of electronic mail

messages have said particular content, generating criteria that classifies electronic

mail messages that have said particular content as a first type of electronic

mail;...

Applicant admits that the cited art teaches that similarity to content of a set of email

messages is used as criteria for classifying other electronic mail messages. However, the cited art

fails to suggest in any way the particular claimed way of automatically determining what

particular electronic mail message's content to use as criteria for classifying electronic mail

messages. Specifically, the cited art fails to suggest in any way generating criteria that classifies

electronic mail messages that have the particular content as a first type of electronic mail by

automatically determining that a threshold number of electronic mail messages contain that

content. More specifically, the cited art fails to suggest in any way "determining that a threshold

number of said plurality of electronic mail messages have a particular content", and "in response

to" making this determination, "generating criteria that classifies electronic mail messages that

have said particular content as a first type of electronic mail."

The Office Action alleges that Leed's teaching about an "authenticator" discloses or

suggests this feature. Applicant admits that the teaching about the authenticator discloses a

system that, like claim 35, uses criteria for classifying an electronic mail message as belonging to

16

a particular type, where the criteria is based on a similarity of the content of the electronic mail

message to the content of electronic mail message that has been determined to belong to that

type. However, the particular way of determining what particular electronic mail message's

content to use for the criteria, where that way is to determine that a threshold number of a

plurality of electronic mail messages have a particular content, is not suggested in any way by

Leeds.

Specifically, the authenticator taught by Leeds determines what particular electronic mail

message's content to use by determining that it has received "negative or adverse notifications

from other users who have received the same or similar emails." Another taught method of

determining what particular electronic mail message's content to use to classify electronic mail

messages includes determining that the sender's address of the electronic mail message is an

undeliverable address (see [0026]). None of these ways taught by Leeds for making a

determination of what particular electronic mail message's content to use as classifying criteria

suggests the claimed way of making such a determination. A determination that "negative or

adverse notifications from other users" about an electronic mail message does not in any way

suggest a determination that a threshold number of said plurality of electronic mail messages

have a particular content, as claimed. A determination that a sender's address of an electronic

mail message is an undeliverable address does not suggest in any way a determination that a

threshold number of said plurality of electronic mail messages have a particular content, as

claimed.

The Office Action also suggests Horvitz's teaching about the use of a threshold value

may be combined with Leeds teaching about basing classifying criteria on the content of

electronic mail messages, the resulting combination suggesting the limitation of:

automatically determining what particular content to use to classify electronic

mail messages by performing steps that include determining that a threshold

number of said plurality of electronic mail messages have a particular content;....

(Office Action, page

However, while Horvitz teaches about using a threshold number or value to classify

electronic mail messages, it is used in a different way than that claimed. Horvitz teaches the

threshold value sets a boundary for an amount of features or content that must be shared with a

set electronic mail message that have been classified as junk mail in order for the electronic mail

message to be classified as junk mail. Claim 35 requires, on the other hand, that the threshold

value set a boundary for the amount of email messages that share a particular content in order to

use that electronic mail messages' content to classify an electronic mail message as a particular

type.

Specifically, Horvitz teaches that electronic mail messages that have a threshold amount

of features or content in the form, for example, of a particular word, can be classified as junk

electronic mail messages. Specifically, "In accordance with our specific inventive teachings,

each incoming e-mail message, in such a stream, is first analyzed to determine which feature(s)

in a set of N predefined features, i.e., distinctions, (where N is an integer), that are particularly

characteristic of spam, the message contains. (i.e., the 'feature set') include both simple-word-

based features and handcrafted features.", (col. 4, lines 54 – 60, see also col. 4, line 67 through

col. 5, line 15) A vector representing the feature set is provided as input to a "probabilistic

classifier, ... which based on the features that are present or absent from the message, generates a

probabilistic measure as to whether that message is spam or not. This measure is then compared

against a preset threshold value. If, for any message, its associated probabilistic measure equals

or exceeds the threshold, then this message is classified as spam..." (col. 9, lines 57 – 68).

18

Thus, as shown above, Horvitz teaches that the threshold value specifies an amount of features or content that an electronic mail message must have in order to be classified as a particular type. Claim 35, on the other hand, requires that the threshold number specify a number of electronic mail messages that must share content in order to use that content **to classify**. In other words, the threshold value of Horvitz only establishes a testing threshold for classifying electronic mail messages; in claim 35, the threshold number establishes a testing threshold for using an electronic mail message to classify.

Furthermore, Horvitz teachings about how to determine what electronic mail messages' content to use to classify electronic mail messages teaches against the automatic claimed way of making this type of determination. Specifically, Horvitz teaches the training set of electronic mail messages from whose content the feature set is derived must be manually classified as junk mail. The "classifier is trained using a set of m e-mail messages (i.e., a "training set", where m is an integer) that have each been **manually** classified as either legitimate or spam." (col. 10; lines 9 – 12) A member of the training set only becomes a member by being classified as spam or legitimate.

Thus, Horvitz teaches to determine what particular electronic mail message's content to use as criteria for classifying electronic mail messages as a particular type by manually classifying the member of the training set as that particular type. Claim 35, on the other hand, requires determining what particular electronic mail message's content to use as criteria for classifying electronic mail messages by automatically determining that a threshold number of electronic mail messages have a particular content. Making a determination of what particular electronic mail message's content to use by manually classifying an electronic mail message does not suggest in any to make such a determination automatically by determining that a threshold number of a set of electronic mail messages have a particular content.

19

The following illustration, based on a comparison between an illustrative embodiment of

claim 35 and embodiments taught by Horvitz and Leeds, demonstrates the differences between

the cited art and the system of claim 35. A sender sends bulk mail message having the following

content: "Sale at Digicams – one half off". In Leeds, Horvitz, and claim 35, the content of the

message is used as criteria that classifies an electronic mail message with the content "Sale at

Digicams – one half off" as bulk mail. However, in Leeds, the determination to use the content

of the bulk mail message to generate criteria is made by determining that "negative or adverse

notifications have been received from other users" about the bulk mail message. In Horvitz, the

determination is made by a user manually adding the email message to a training set. In claim

35, the determination is made by automatically determining that a threshold number of the bulk

mail messages (e.g. 50) have the content "Sale at Digicams – one half off"

As shown above, the cited art fails to disclose or suggest in any way all the limitations of

claim 35. Therefore, claim 35 is patentable. Reconsideration and allowance of claim 35 is

respectfully requested.

NEW CLAIM 37

Claim 37, recites:

wherein at least one message of said plurality of messages has not been classified, before

determining that a threshold number of said plurality of electronic mail messages

have a particular content, as belonging to said first type.

Claim 37 contains all the limitations of claim 35 and is therefore patentable for at least

the reasons claim 35 is patentable. Furthermore, claim 35 adds a limitation that further

distinguishes the cited art's use of the electronic mail message content to classify other electronic

mail messages as a particular type. For example, assuming Horvitz teaches using content of

20

electronic mail messages in the training set to generate criteria for classifying electronic mail messages, Horvitz teaches that the determination that triggers the use of a particular electronic mail messages' content to generate criteria must be made only after the electronic mail messages have been manually classified by a user as a particular type of electronic mail message. In claim 35, the determination that triggers the use of an electronic mail message's content to generate criteria is not only made only if the electronic mail message has been classified as a particular type of electronic mail message.

<div align="center">CLAIMS 15 AND 31</div>

Claims 15 and 31, recite:

a central server receiving from a set of electronic mail servers message signatures

generated from electronic mail messages received by said set of electronic mail

servers, wherein each message signature includes one or more signature elements;

said central server generating counts of how many times said one or more signature

elements are matched by signature elements from message signatures generated

for other electronic mail messages;

The cited art fails to disclose or suggest in any way all the limitations of claims 15 and 31. For example, the cited art fails to disclose or suggest in any way the limitation of "counts of how many times said one or more signature elements are **matched** by signature elements from message signatures generated for other electronic mail messages."

The Office Action has equated the message signatures received to the digital signatures in electronic mail message received by the system taught by Leeds (see Office Action, page 9, line 10 - 12). Furthermore, the Office Action alleges that the teaching at paragraph [0024] about assigning confidence ratings to electronic mail messages teaches about generating counts of matching signatures elements of electronic mail messages. Thus, it appears that the Office

<div align="center">21</div>

Action is also equating signature elements to confidence ratings and alleging that paragraph [0024] teaches generating counts of how many signature elements from mail messages are matched.

Regardless of whether the digital signatures or the confidence ratings have been equated to the signature elements claimed, this paragraph fails to suggest in any way much less disclose generating a count of matching confidence scores or matching digital signatures. Paragraph [0024] is shown below.

The method and system of the present invention assign confidence ratings to messages to signify the statuses of the messages as junk e-mails or as a bona fide messages that the recipient may wish to read. The method and system begin by analyzing the origins and transmission paths of the messages. The sender's origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent. Based on the verification response that is received in response to the verification request, the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail. Incoming messages (e-mails) are automatically scanned and parsed, either (1) at a server located at an Internet provider (prior to delivery to the intended ultimate recipient), (2) at a LAN-based receiving station, or (3) at the actual ultimate recipient's mail machine, i.e., local to the user. Once the message has been parsed or broken down into fields, the message is compared with several user defined rules for handling messages, and a confidence rating is assigned to the message. In one embodiment, the message header information is analyzed and a verification request(s) is/are automatically sent to the purported sender(s), as identified by fields such as "From:" or "Reply-To:". If there is a delivery problem

22

in delivering the verification request, the presumed validity of the message is reduced in accordance with a set of user-definable criteria. In addition to determining the purported origination point, the present invention automatically analyzes all information pertaining to the sender, the path of delivery, any information pertaining to copies, blind copies, or other indicia of validity of the origin of the message to determine if there has been a discernable effort to obscure the origin, disguise the sender, or in some other way to inhibit the recipient from performing verification of the sender's identity. For example, if a message has purportedly been relayed through a machine named mail.fromnowhere.com and the mail handling system has determined that such a machine does not actually exist, the confidence rating for the message should be decreased. (Leeds, 0024)

As is easily discerned above by a careful reading of the paragraph, the confidence rating assigned is generated based on determining that the sender's address of an electronic mail message is an undeliverable and applying "several user defined rules for handling messages." There is nothing however in this passage to suggest in any way that the confidence rating assigned to an email is compared to other confidence ratings assigned other emails to determine whether it matches confidence ratings of the other electronic mail messages, let alone that a count is made of how many confidence ratings match. There is also nothing in the paragraph that discusses operations concerning a digital signature of an electronic mail message, let alone comparing the digital signature with digital signatures of other electronic mail messages and determining a count of those that match.

23

Finally, the Office Action alleges that Leeds teaches "transmitting a message that reflects the counts" because a message reflecting counts is inherent when counting is involved in tracking how many signature elements there are. The message claimed reflects a count of how many signature elements are matched. This is not necessarily implied by how many signature elements there are. Furthermore, Leeds does not even teach tracking "tracking how many signature elements there are."

CLAIMS 1 AND 26

Claims 1 and 26 recite:

automatically generating a set of criteria based on contents of a plurality of electronic
mail messages received over a network;

**wherein the step of automatically generating a set of criteria includes, in response to
determining that a threshold number of said plurality of electronic mail
messages have a particular content, generating criteria that classifies
electronic mail messages that have said particular content as a first type of
electronic mail;...**

As mentioned before, Leeds and Horvitz describe a system that classifies electronic mail messages based on particular content contained therein, where the particular content has been predetermined to be indicative of junk mail. For example, Leeds teaches that electronic mail messages that include certain phrases and keywords in the message body (0026, 0034) can be classified as junk electronic mail messages. Horvitz teaches that electronic mail messages that have particular content in the form of, for example, particular words can be classified as junk electronic mail messages. (col. 4, lines 54 – 60, "In accordance with our specific inventive teachings, each incoming e-mail message, in such a stream, is first analyzed to determine which

24

feature(s) in a set of N predefined features, i.e., distinctions, (where N is an integer), that are particularly characteristic of spam, the message contains. These features (i.e., the 'feature set') include both simple-word-based features and handcrafted features.")

While the cited art teaches using particular content as criteria for classifying the electronic mail messages, it fails to suggest in any way the particular claimed way of determining what particular content to use as criteria for classifying electronic mail messages, and in particular, fails to suggest in any the claimed way of automatically determining that particular content is contained in a threshold number of electronic mail messages, and in response, generating criteria that classifies electronic mail messages that have the particular content as a first type of electronic mail. Specifically, it fails to suggest in any way "determining that a threshold number of said plurality of electronic mail messages have a particular content", and "in response to" making this determination, "generating criteria that classifies electronic mail messages that have said particular content as a first type of electronic mail."

As shown above, the cited art does not disclose or suggest in any way all the limitations of claims 1 and 26. Therefore, claims 1 and 26 are patentable. Reconsideration and allowance of claims 1 and 26 is respectfully requested.

CLAIMS 10 AND 29

Claims 10 and 29, as amended, recite:

an electronic mail server determining whether said message signature satisfies a set of
    criteria based on message signatures previously received by said central server
    from a set of electronic mail servers; and
wherein said set of criteria classifies said electronic mail message and a threshold number
    of electronic mail messages as having a particular content;...

25

The cited art fails to disclose or suggest in any way all the limitations of claims 10 and 29, recited above. As stated with respect to limitations in claims 1 and 26, the cited art fails to disclose or suggest in any way "generating criteria that classifies electronic mail messages that have [a] particular content as a first type of electronic mail" "in response to determining that a threshold number of said plurality of electronic mail messages have [the] particular content". For similar reasons, the cited art would also fail to disclose or suggest in any way "an electronic mail server determining whether said message signature satisfies a set of criteria based on message signatures previously received", where the "set of criteria [that is] based on the message signatures previously received" is used to "[classify] said electronic mail message and a threshold number of electronic mail messages as having a particular content." Therefore, claims 10 and 29 are patentable. Reconsideration and allowance of claims 10 and 29 is respectfully requested.

CLAIMS 19 AND 32

Claims 19 and 32 recite:

determining whether said message signature satisfies a set of criteria that indicates said
electronic mail message and a threshold number of electronic mail messages have
a particular content;...

The cited art fails to disclose or suggest in any way all the limitations of claims 19 and 32. For example, the cited art fails to disclose or suggest in any way the limitation of "determining whether said message signature satisfies a set of criteria that indicates said electronic mail message and a threshold number of electronic mail messages have a particular content". As stated with respect to limitations in claims 1 and 26, the cited art fails to disclose or suggest, "generating criteria that classifies electronic mail messages that have [a] particular content as a first type of electronic mail" "in response to determining that a threshold number of

26

said plurality of electronic mail messages have [the] particular content". For similar reasons, the

cited art would also fail to disclose or suggest in any way "determining whether said message

signature satisfies a set of criteria that indicates said electronic mail message and a threshold

number of electronic mail messages have a particular content", as claimed. Therefore, claims 19

and 32 are patentable. Reconsideration and allowance of claims 19 and 32 is respectfully

requested.

DEPENDANT CLAIMS

The pending claims not discussed so far are dependant claims that depend on an

independent claim that is discussed above. Because each of the dependant claims include the

limitations of claims upon which they depend, the dependant claims are patentable for at least

those reasons the claims upon which the dependant claims depend are patentable. In addition, the

dependent claims introduce additional limitations that independently render them patentable.

However, due to fundamental differences already identified, the additional limitations are not
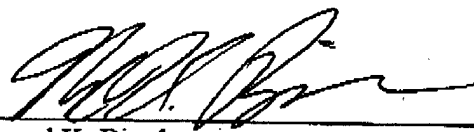
discussed at this time.

For the reasons set forth above, Applicant respectfully submits that all pending claims are patentable over the art of record, including the art cited but not applied. Accordingly, allowance of all claims is hereby respectfully solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: August 12, 2003

Marcel K. Bingham
Reg. No. 42,327

RECEIVED

AUG 1 4 2003

Technology Center 2100

1600 Willow Street
San Jose, CA 95125
Telephone No.: (408) 414-1080 ext.206
Facsimile No.: (408) 414-1076

OFFICIAL

CERTIFICATE OF TRANSMISSION
I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office Fax No. (703) 746-7238

on   8/12/03   by   Trudy Bragdon

28